

Folding Alternant and Goppa Codes with Non-Trivial Automorphism Groups

Jean-Charles Faugère^{†*‡}, Ayoub Otmani[§], Ludovic Perret^{*†‡}, Frédéric de Portzamparc^{*†‡||} and Jean-Pierre Tillich[¶]

*Sorbonne Universités, UPMC Univ Paris 06, POLSYS, UMR 7606, LIP6, F-75005, Paris, France
ludovic.perret@lip6.fr

[†] INRIA, Paris-Rocquencourt Center,
jean-charles.faugere@inria.fr

[‡] CNRS, UMR 7606, LIP6, F-75005, Paris, France

[§] Normandie Univ, France; UR, LITIS, F-76821 Mont-Saint-Aignan, France.
ayoub.otmani@univ-rouen.fr.

[¶]INRIA, Paris-Rocquencourt Center,
jean-pierre.tillich@inria.fr

^{||}Gemalto, 6 rue de la Verrerie 92190, Meudon, France
frederic.urvoydeportzamparc@gemalto.com

Abstract

The main practical limitation of the McEliece public-key encryption scheme is probably the size of its key. A famous trend to overcome this issue is to focus on subclasses of alternant/Goppa codes with a non trivial automorphism group. Such codes display then *symmetries* allowing compact parity-check or generator matrices. For instance, a key-reduction is obtained by taking *quasi-cyclic* (QC) or *quasi-dyadic* (QD) alternant/Goppa codes. We show that the use of such *symmetric* alternant/Goppa codes in cryptography introduces a fundamental weakness. It is indeed possible to reduce the key-recovery on the original symmetric public-code to the key-recovery on a (much) smaller code that has not anymore symmetries. This result is obtained thanks to a new operation on codes called *folding* that exploits the knowledge of the automorphism group. This operation consists in adding the coordinates of codewords which belong to the same orbit under the action of the automorphism group. The advantage is twofold: the reduction factor can be as large as the size of the orbits, and it preserves a fundamental property: folding the dual of an alternant (*resp.* Goppa) code provides the dual of an alternant (*resp.* Goppa) code. A key point is to show that all the existing constructions of alternant/Goppa codes with symmetries follow a common principal of taking codes whose support is globally invariant under the action of affine transformations (by building upon prior works of T. Berger and A. Dür). This enables not only to present a unified view but also to generalize the construction of QC, QD and even *quasi-monoidic* (QM) Goppa codes. All in all, our results can be harnessed to boost up any key-recovery attack on McEliece systems based on symmetric alternant or Goppa codes, and in particular algebraic attacks.

I. INTRODUCTION

Some significant research efforts have been put recently in code-based cryptography to reduce by a large factor the public key sizes. This has resulted in keys which are now only a few times larger than RSA keys (see [1], [2] for instance). This is obtained by focusing on codes having *symmetries*, that is to say, codes having a non-trivial automorphism group. Such codes have the advantage of admitting a compact parity-check or generator matrix [3], [4], [5], [1], [6]. Quasi-cyclic (QC) codes represent a good example of the use of symmetries in cryptography to build public-key encryption schemes with short keys [3], [4]. It was then followed by a series of papers proposing alternant and Goppa codes with different automorphism groups like quasi-dyadic (QD) Goppa or Srivastava codes [5], [6] and quasi-monoidic (QM) codes [1]. The rationale behind this is the fact that the additional structure does not

A preliminary version of this paper will be presented at ISIT'14 under the title "Structural Weakness of Compact Variants of the McEliece Cryptosystem".

deteriorate the security of the cryptographic scheme. This hope was eroded by the apparition of specific attacks [7], [8] and algebraic attacks [9], [10], [11] against QC/QD alternant/Goppa codes. Despite these preliminary warning signals, the design of compact McEliece schemes remains a rather popular topic of research e.g. [12], [1], [6], [13], [14]. Besides these cryptographic motivations, the search for Goppa codes, and more generally alternant codes, with non-trivial automorphisms is in itself an important issue in coding theory. Several papers focused on the problem of constructing quasi-cyclic Goppa codes [15], [16], or identifying alternant and Goppa codes invariant under a given permutation [17], [18], [19].

Main Results

All the constructions of *symmetric* alternant/Goppa codes presented in previous works might look at first glance unrelated, like *ad hoc* constructions designed for a very specific goal. In [5] symmetric QD Goppa codes are constructed by using the narrower class of separable Goppa codes which have all their roots of multiplicity one in the field over which the coefficients of the Goppa polynomial are taken and by choosing these roots in an appropriate manner; the same approach is followed to obtain more general QM Goppa codes in [1], whereas in [4] the authors rely on the larger class of alternant codes to obtain a large enough family of QC codes in a McEliece like scheme. Building upon the work of [20], [19], [18], we show in this paper that all the QC, QD and QM alternant/Goppa codes which are constructed in [4], [5], [1] rely actually on a common principle (Proposition 3). They are all equipped with non-trivial automorphism groups that involve some affine transformations leaving globally invariant their support. This property imposes on the non-zero scalars defining the alternant codes the constraint of being built from a root of unity. In the case of Goppa codes, this constraint is translated into a *functional equation* of the form $\alpha\Gamma(az + b) = \Gamma(z)$ that the Goppa polynomial $\Gamma(z)$ has to satisfy, where α is a root of unity and a, b belong to the underlying finite field on which the support is defined. We fully characterize polynomials satisfying such equation in Proposition 4. This enables not only to present a unified view but also to generalize the construction of QC, QD and QM Goppa codes (Proposition 5). In particular, there is no need to use separable polynomials like in [5] for getting QD Goppa codes. Notice that this will also show that it is in principle not compulsory to take the larger family of alternant codes instead of Goppa codes as in [4] to obtain a large enough family of QC codes in a McEliece scheme: in fact there is nothing special with respect to QD Goppa codes instead of QC Goppa codes because there are roughly as many QD Goppa codes as there are QC Goppa codes (for a same size of automorphism group) with our way of constructing them.

The major contribution of our paper is to prove that alternant and Goppa codes with symmetries can be seen as an *inflated* version of a smaller alternant code *without* symmetries. We call this latter a *folded* code because we show that it can be obtained easily by adding the coordinates which belong to the same orbit under the action of a permutation of the automorphism group. More importantly, we can also express precisely the relationship between the supports and the non-zero scalars defining the alternant/Goppa with symmetries and their associated folded codes. These links are so explicit for the non-zero scalars that knowing those of the folded code is sufficient for knowing those of the original symmetric alternant/Goppa codes. These results have an important impact in cryptography. First the length and the dimension of the folded code is generally divided by the cardinality of the automorphism group. It means in particular that the use of compact alternant/Goppa codes introduces a fundamental weakness: decreasing the size of the public-key as in [4], [5], [1] necessarily implies a deterioration of the security. Furthermore, since the non-zero scalars of the folded code bear crucial information, it then allows in the context of algebraic attacks as proposed in ([9], [10], [21]), to reduce a key-recovery attack on the original public-code to the one on a smaller code, that is to say with less variables in the polynomial system. For instance, we can reduce the key-recovery of a quasi-dyadic Goppa code of length 8192 and dimension 4096 to the key-recovery on a Goppa code of length 64 and dimension 32.

Interestingly enough, the folded code, if used in a McEliece-like encryption scheme, would have the same key size as the original scheme but without symmetries. In other words, the very reason which allowed to reduce the key size in [4], [5], [1], [13] can be used to derive a *reduced* McEliece scheme whose key-recovery hardness and key size is equivalent to the original system.

Comparison with “Structural Cryptanalysis of McEliece Schemes with Compact Keys” [21]

This paper is a companion paper of [21] which has been submitted separately. In [21], we mainly focused on the cryptanalysis of QM Goppa codes. That is, we [21] developed new algebraic tools for solving the algebraic systems arising in the cryptanalysis QM Goppa codes, reported various experimental results and prove in addition partial results on folded QM Goppa codes. In this submission, we present a much deeper and more systematic treatment of the the folding process. In [21], the folding was performed directly over QM Goppa codes and it was proved there that it results in a subcode of a Goppa code of reduced length. Using a slightly different approach (by considering the dual of the codes), we obtain here a much stronger result which holds in a more general setting. Namely, we prove that if we perform folding on the dual of QC, QD or QM affine induced Goppa/alternant codes (this applies for instance to all the codes constructed in [4], [5], [13], [1]) we obtain a reduced dual Goppa or alternant code where the reduction factor can be as large as the size of the cyclic or monodic blocks of a symmetric parity-check matrix attached to these codes. Folding preserves here the structure of the dual code: if we start with the dual of an alternant code we end up with the dual of an alternant code and if we start with the dual of a Goppa code we end up with the dual of a Goppa code.

II. ALTERNANT AND GOPPA CODES

In this section we introduce notation which is used in the whole paper and recall a few well known facts about alternant and Goppa codes. Throughout the paper, the finite field of q elements with q being a power of a prime number p is denoted by \mathbb{F}_q . Vectors are denoted by bold letters like \mathbf{x} and the notation $\mathbf{x} = (x_i)_{0 \leq i < n}$ or $\mathbf{x} = (x_i)_{i=0}^{n-1}$ will be used in some cases. The ring of polynomials with coefficients in a finite field \mathbb{F} is denoted by $\mathbb{F}[z]$, while the subspace of $\mathbb{F}[z]$ of polynomials of degree less than t (resp. less than or equal to t) is denoted by $\mathbb{F}[z]_{<t}$ (resp. $\mathbb{F}[z]_{\leq t}$). When $\mathbf{x} = (x_i)_{0 \leq i < n}$ is a vector in \mathbb{F}^n and $Q(z)$ is a polynomial in $\mathbb{F}[z]$, $Q(\mathbf{x})$ stands for $(Q(x_0), \dots, Q(x_{n-1}))$. In particular for any vector $\mathbf{u} = (u_0, \dots, u_{n-1})$ and for all $a, b \in \mathbb{F}$ then $a\mathbf{u} + b$ stands for the vector $(au_0 + b, \dots, au_{n-1} + b)$.

Definition 1 (Generalized Reed-Solomon code) Let q be a prime power and k, n be integers such that $1 \leq k < n \leq q$. Let \mathbf{x} and \mathbf{y} be two n -tuples such that the entries of \mathbf{x} are pairwise distinct elements of \mathbb{F}_q and those of \mathbf{y} are nonzero elements in \mathbb{F}_q . The generalized Reed-Solomon code $\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$ of dimension k is the k -dimensional vector space:

$$\mathbf{GRS}_k(\mathbf{x}, \mathbf{y}) \stackrel{\text{def}}{=} \left\{ (y_0 P(x_0), \dots, y_{n-1} P(x_{n-1})) \mid P \in \mathbb{F}_q[z]_{<k} \right\}.$$

A useful property of these codes is given in [22, Chap. 12, §2].

Proposition 1 Keeping the notation of Definition 1, there exists a vector $\mathbf{z} \in \mathbb{F}_q^n$ such that $\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})^\perp = \mathbf{GRS}_{n-k}(\mathbf{x}, \mathbf{z})$.

This leads to the definition of alternant codes.

Definition 2 (Alternant code, degree, support, multiplier) Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^m}^n$ be two vectors such that the entries of \mathbf{x} are pairwise distinct and those of \mathbf{y} are all nonzero, and let r and m be positive integers. The alternant code $\mathcal{A}_r(\mathbf{x}, \mathbf{y})$ defined over \mathbb{F}_q is the subfield subcode over \mathbb{F}_q of $\mathbf{GRS}_r(\mathbf{x}, \mathbf{y})^\perp \subset \mathbb{F}_{q^m}^n$:

$$\mathcal{A}_r(\mathbf{x}, \mathbf{y}) \stackrel{\text{def}}{=} \mathbf{GRS}_r(\mathbf{x}, \mathbf{y})^\perp \cap \mathbb{F}_q^n.$$

The integer r is the degree of the alternant code, \mathbf{x} is a support and \mathbf{y} is a multiplier of the alternant code.

The dual of a subfield subcode is known to be a trace code [23]. From this it follows that

Lemma 1 The dual $\mathcal{A}_r(\mathbf{x}, \mathbf{y})^\perp$ of the alternant code $\mathcal{A}_r(\mathbf{x}, \mathbf{y})$ of degree r and extension m over \mathbb{F}_q is given by:

$$\mathcal{A}_r(\mathbf{x}, \mathbf{y})^\perp = \text{Tr} \left(\mathbf{GRS}_r(\mathbf{x}, \mathbf{y}) \right) = \left\{ (\text{Tr}(c_0), \dots, \text{Tr}(c_{n-1})) \mid (c_0, \dots, c_{n-1}) \in \mathbf{GRS}_r(\mathbf{x}, \mathbf{y}) \right\}$$

where Tr is the trace map from \mathbb{F}_{q^m} to \mathbb{F}_q defined by $\text{Tr}(z) = z + z^q + \dots + z^{q^{m-1}}$.

Let us remark that an alternant code has many equivalent descriptions as shown by the following proposition whose proof can be found in [22, Chap. 10, p. 305].

Proposition 2 *For all $a \in \mathbb{F}_{q^m} \setminus \{0\}$, $b \in \mathbb{F}_{q^m}$, and $c \in \mathbb{F}_{q^m} \setminus \{0\}$, it holds that:*

$$\mathcal{A}_r(\mathbf{x}, \mathbf{y}) = \mathcal{A}_r(a\mathbf{x} + b, c\mathbf{y}).$$

We introduce now Goppa codes which form an important subfamily of alternant codes.

Definition 3 (Classical Goppa codes) *Let $\mathbf{x} = (x_0, \dots, x_{n-1})$ be an n -tuple of distinct elements of \mathbb{F}_{q^m} and choose $\Gamma(z) \in \mathbb{F}_{q^m}[z]$ of degree r such that $\Gamma(x_i) \neq 0$ for all $i \in \{0, \dots, n-1\}$. The Goppa code $\mathcal{G}(\mathbf{x}, \Gamma)$ of degree r over \mathbb{F}_q associated to $\Gamma(z)$ is the alternant code $\mathcal{A}_r(\mathbf{x}, \mathbf{y})$ with*

$$y_i = \frac{1}{\Gamma(x_i)}.$$

$\Gamma(z)$ is called the Goppa polynomial and \mathbf{x} is the support of the Goppa code.

III. CONSTRUCTION OF SYMMETRIC ALTERNANT AND GOPPA CODES

The purpose of this section is to recall how quasi-cyclic (QC), quasi-dyadic (QD) and quasi-monoidic (QM) alternant/Goppa codes [5], [13], [1] and more generally any *symmetric* alternant/Goppa code can be constructed from a common principle which stems from Dür's work in [20] about the automorphism group of (generalized) Reed-Solomon codes. This has been applied and developed in [19], [18] to construct large families of symmetric alternant or Goppa codes. It should be emphasized that this way of constructing symmetric Goppa codes is more general than the constructions proposed for QD or QM Goppa in a cryptographic context by [5], [13], [1]. In particular, it is required in [5], [13], [1] to choose Goppa codes with a separable Goppa polynomial. We will prove in the following that this constraint is unnecessary.

In order to recall these results we need a few definitions. An *automorphism* of a code of length n defined over \mathbb{F}_q is an isometry of the Hamming space \mathbb{F}_q^n i.e. a linear transform of \mathbb{F}_q^n which both preserves the Hamming weight and leaves the code globally invariant. A well-known fact about such isometries is that they consist of permutations and/or non-zero multiplications of the coordinates.

In this paper, we will be interested only in isometries that are permutations. This action is denoted, given a permutation σ of the symmetric group on $\{0, \dots, n-1\}$ and a vector $\mathbf{x} = (x_0, \dots, x_{n-1})$, by $\mathbf{x}^\sigma \stackrel{\text{def}}{=} (x_{\sigma(0)}, \dots, x_{\sigma(n-1)})$. For a code \mathcal{C} and a permutation σ , we define:

$$\mathcal{C}^\sigma \stackrel{\text{def}}{=} \{\mathbf{c}^\sigma \mid \mathbf{c} \in \mathcal{C}\}.$$

A *permutation automorphism* of \mathcal{C} is then any permutation σ such that \mathbf{c}^σ is in \mathcal{C} whenever \mathbf{c} belongs to \mathcal{C} . *Symmetric codes* are then codes with a *non-trivial* automorphism group.

We have seen in Proposition 2 that alternant codes may have several identical descriptions thanks to affine transformations. Actually, symmetric Goppa codes and alternant codes can easily be constructed by looking at the action of the projective semi-linear group on the support of these codes as shown in [19], [18]. By projective semi-linear group, we mean here transformations of the form:

$$\begin{aligned} \mathbb{F}_{q^m} \cup \{\infty\} &\rightarrow \mathbb{F}_{q^m} \cup \{\infty\} \\ z &\mapsto \frac{az^{q^i} + b}{cz^{q^i} + d} \end{aligned}$$

Basically when the support of the alternant code is invariant by the action of such a transformation and under a certain condition on the multiplier, it turns out that such a transformation induces a permutation automorphism of the alternant code. However, this action on the support may transform a coordinate of the support into ∞ and a slightly more general definition of generalized Reed-Solomon codes and of alternant codes is required to cope with this issue. This is why A. Dür introduced Cauchy codes in [20] which are in essence a further generalization of

generalized Reed-Solomon codes. This construction allows to have ∞ in its support. To avoid such a technicality (and also to simplify some of the statements and propositions obtained here) we will only consider the subgroup of affine transformations of the projective semi-linear group. It should be noted however that this simplification permits to cover all the constructions of symmetric alternant or Goppa codes used in a cryptographic context [4], [5], [13], [1], [6] and in some cases even to generalize them. Namely, we will deal with the following cases:

Definition 4 Let \mathcal{C} be an alternant or Goppa code defined over a field \mathbb{F} of length n , with an automorphism group \mathbb{G} . Given a nonnegative integer $\lambda \leq n$, we say that \mathcal{C} is:

- *Quasi-Cyclic (QC)* if \mathbb{G} is of the form $(\mathbb{Z}/\lambda\mathbb{Z})$,
- *Quasi-Dyadic (QD)* if $\text{char}(\mathbb{F}) = 2$ and \mathbb{G} is of the form $(\mathbb{Z}/2\mathbb{Z})^\lambda$,
- *Quasi-Monoidic (QM)* if \mathbb{G} is of the form $(\mathbb{Z}/p\mathbb{Z})^\lambda$ with $p = \text{char}(\mathbb{F}) > 2$.

Let us now reformulate some corollaries of the results obtained in [19], [18] in this particular case. The symmetric alternant or Goppa codes that will be obtained here correspond to permutation automorphisms of alternant or Goppa codes based on the action of affine maps $x \rightarrow ax + b$ on the support $(x_0, x_1, \dots, x_{n-1})$ of the Goppa code or the alternant code. If this support is globally invariant by this affine map (and a is not equal to 0), then this induces a permutation σ of the code positions $\{0, 1, \dots, n-1\}$ by defining $\sigma(i)$ as the unique integer in $\{0, 1, \dots, n-1\}$ such that $x_{\sigma(i)} = ax_i + b$. In such a case, we say that σ is the *permutation induced by the affine map* $x \rightarrow ax + b$. Restricting Theorem 1 of [18] to affine transformations yields immediately

Proposition 3 Let $a \neq 0$ and b be elements of \mathbb{F}_{q^m} . Let $\mathbf{x} \in \mathbb{F}_{q^m}^n$ be a support which is globally invariant by the affine map $x \rightarrow ax + b$. Let σ be the permutation of S_n induced by this affine map. Let ℓ be the order of σ . Assume that $\mathbf{y} \in (\mathbb{F}_{q^m})^n$ is an n -tuple of nonzero elements such that $\exists \alpha \in \mathbb{F}_{q^m}$ an ℓ -th root of unity such that $y_{\sigma(i)} = \alpha y_i$, for all $i \in \{0, 1, \dots, n-1\}$. Then σ is a permutation automorphism of the alternant code $\mathcal{A}_t(\mathbf{x}, \mathbf{y})$ for any degree $t > 0$.

If we want to obtain Goppa codes, we can apply this result and we just have to check that the conditions on the support $x_{\sigma(i)} = ax_i + b$ and multiplier $y_{\sigma(i)} = \alpha y_i$ are compatible with the definition of the Goppa code, namely $y_i = \frac{1}{\Gamma(x_i)}$ where $\Gamma(x)$ is the Goppa polynomial. These considerations yield immediately the following corollary of Proposition 3.

Corollary 1 Let $a \neq 0$ and b be elements of \mathbb{F}_{q^m} with $b \neq 0$ when $a = 1$. Let $\mathbf{x} \in \mathbb{F}_{q^m}^n$ be a support which is globally invariant by the affine map $x \rightarrow ax + b$. Let σ be the permutation of S_n induced by this affine map and let ℓ be its order. Assume that there exists a polynomial $\Gamma(z)$ and an ℓ -th root of unity α in \mathbb{F}_{q^m} which is such that

$$\Gamma(az + b) = \alpha \Gamma(z). \quad (1)$$

In such a case, σ is a permutation automorphism of the Goppa code $\mathcal{G}(\mathbf{x}, \Gamma)$.

This proposition allows to obtain easily Goppa codes or alternant codes with a non trivial automorphism group that is cyclic.

Remark 1 One might wonder whether it is possible to characterize polynomials which satisfy Equation (1). In [19, Theorem 4] a slightly more general polynomial equation is considered, namely $\Gamma(az^{q^s} + b) = \alpha \Gamma(z)^{q^s}$. It is the particular case of $s = m$ of Theorem 4 of [19] which is of interest to us here. However, since it deals with the classification of cyclic alternant codes (there is therefore a restriction on the order compared to the length which trivializes the solutions of this problem in many cases which are of interest to us) and since for further purposes it will be convenient for us to remove the assumption on $\Gamma(z)$ to have no roots in $\{x_0, \dots, x_{n-1}\}$ which is done implicitly in Theorem 4 (and also in Lemma 2 of [19] that is used to prove Theorem 4) we can not use it in our case directly.

The characterization of the solution set to (1) we will use is the following.

Proposition 4 Let \mathbb{F} be a field of finite characteristic p and let a, b, α be elements of \mathbb{F} , such that (i) $a \neq 0$ and (ii) $b \neq 0$ when $a = 1$. All the polynomials $\Gamma(z) \in \mathbb{F}[z]$ satisfying $\Gamma(az + b) = \alpha\Gamma(z)$ have the following form

- If $a = 1$ then necessarily $\alpha = 1$, $\ell = p$ and $\Gamma(z)$ is any polynomial in $\mathbb{F}[z]$ of degree a multiple of p which is of the form $\Gamma(z) = P(z^p - bz^{p-1})$.
- If $a \neq 1$ then there exists a unique integer d in the range $[0, \dots, \ell - 1]$ such that $\alpha = a^d$ and if we denote by z_0 the unique fixed point of the affine map $z \rightarrow az + b$, we have that $\Gamma(z)$ is any polynomial in $\mathbb{F}[z]$ of degree equal to d modulo ℓ which is of the form $(z - z_0)^d P((z - z_0)^\ell)$.

The proof of this proposition can be found in Appendix A. By taking polynomials P in this proposition which are such that the resulting $\Gamma(z)$ has no zeros in the support (x_0, \dots, x_{n-1}) we obtain Goppa codes with a cyclic permutation automorphism group. To obtain automorphism groups which are isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\lambda$, for some $\lambda \geq 1$, we need a slightly more general statement which is the following:

Proposition 5 Let $p \stackrel{\text{def}}{=} \text{char}(\mathbb{F}_{q^m})$. Let $\alpha_0, \dots, \alpha_{\lambda-1} \in \mathbb{F}_{q^m}$ be a set of s elements which are \mathbb{F}_p -independent over \mathbb{F}_{q^m} . Let G be the group of order p^λ generated by the α_i 's. Consider a support $\mathbf{x} \stackrel{\text{def}}{=} (x_0, \dots, x_{n-1})$ which is globally invariant by all the affine transformations $z \rightarrow z + \alpha_i$ and assume that the multiplier $\mathbf{y} \stackrel{\text{def}}{=} (y_0, y_1, \dots, y_{n-1})$ is constant on the cosets of G meaning that $y_i = y_j$ iff $x_i - x_j \in G$. Then $\mathcal{A}_r(\mathbf{x}, \mathbf{y})$ is an alternant code with a permutation automorphism group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\lambda$ for any degree r . Let $P(z) \stackrel{\text{def}}{=} \prod_{g \in G} (z - g)$, then any polynomial $\Gamma(z)$ of the form $\Gamma(z) = Q(P(z))$ where Q is a polynomial in $\mathbb{F}_{q^m}[z]$ gives a Goppa code $\mathcal{G}(\mathbf{x}, \Gamma(z))$ of degree $p^\lambda \deg Q$ with an automorphism group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\lambda$.

Proof: All the shifts $z \rightarrow z + \alpha_i$ give rise to a permutation automorphism of the alternant code by Proposition 3 and they generate a group of order p^λ from the independence assumption on the α_i 's. The statement about Goppa codes follows by observing that the polynomial $\Gamma(z) = Q(\prod_{g \in G} (z - g))$ is invariant by all the shifts $z \rightarrow z + \alpha_i$ and by using Corollary 1. ■

Remark 2 1) A support (x_0, \dots, x_{n-1}) satisfying the conditions of Proposition 5 is easily obtained by taking unions of cosets of G and getting a QD or a QM Goppa code is obtained by arranging the support as follows. We define $\mathbf{x} = (x_i)_{0 \leq i < n}$ by choosing elements $x_0, x_{p^\lambda}, \dots, x_{(n_0-1)p^\lambda}$ in different cosets of \mathbb{F}_{q^m}/G (where $n = n_0 p^\lambda$). The remaining x_i 's are chosen as follows:

$$x_i = x_{\lfloor i/p^\lambda \rfloor p^\lambda} + \sum_{j=0}^{\lambda-1} i_j \alpha_j. \quad (2)$$

It is readily checked that all the QD or QM constructions of Goppa codes of [5], [13], [1] are just special cases of this construction. It should be observed that the construction presented here is more general. In particular, $\Gamma(z)$ does not need to split over \mathbb{F}_{q^m} as in [5], [13], [1]. It may even be irreducible as shown by the example $p = q = 2$, $G = \mathbb{F}_2$, m odd and $\gamma(z) = 1 + z$.

- 2) By using our proof technique of Proposition 4 it can actually be shown that all polynomials $\Gamma(z)$ invariant by the shifts $z \rightarrow z + \alpha_i$ are actually polynomials of the form $Q(\prod_g (z - g))$.

From now on, we will say that the permutation automorphism group of an alternant code or a Goppa code that is obtained by such affine maps (be it a single affine map or a collection of them) is the *permutation group induced* by such affine maps. As observed in [18], an alternant code or a Goppa code can be invariant by a permutation which is not induced by an affine map or more generally by an element of the projective semilinear group. However, there is no general way of constructing this kind of permutation and it should also be noted that in the case of GRS or Cauchy codes, the whole permutation group is actually induced by the projective linear group, i.e. the set of transformations of the kind $z \rightarrow \frac{az+b}{cz+d}$ (this is actually a consequence of Theorem 4 of [20]).

IV. AFFINE-INVARIANT POLYNOMIALS

The key ingredient which allows to reduce to smaller alternant codes or Goppa codes when these are either quasisystematic or quasi-cyclic is a fundamental result on the form taken by polynomials which are invariant by an affine

map. These polynomials will arise as sums of the form:

$$Q(z) \stackrel{\text{def}}{=} \sum_{i=0}^{\ell-1} \alpha^i P(\sigma^i(z)) \quad (3)$$

where P is a polynomial, σ an affine map of order ℓ and α an ℓ -th root of unity. Such polynomial sums clearly satisfy polynomial Equation (1), since:

$$\begin{aligned} Q(\sigma(z)) &= \sum_{i=0}^{\ell-1} \alpha^i P(\sigma^{i+1}(z)) = \frac{1}{\alpha} \sum_{i=0}^{\ell-1} \alpha^{i+1} P(\sigma^{i+1}(z)) \\ &= \frac{1}{\alpha} \sum_{i=0}^{\ell-1} \alpha^i P(\sigma^i(z)) = \frac{1}{\alpha} Q(z). \end{aligned}$$

Proposition 4 characterizes all solutions of the polynomial Equation (1). Conversely, and this will be crucial in our context, it turns out that all these solutions are of the form (3). To formalize this point, we introduce the following notation

Notation 1 Let $I_{\leq t}^{\sigma, \alpha}[z] \subseteq \mathbb{F}_{\leq t}[z]$ be the set of polynomials of degree $\leq t$ which satisfy (1), i.e. which satisfy $P(\sigma(z)) = \alpha P(z)$. When $\alpha = 1$ we will simply write $I_{\leq t}^{\sigma}[z]$. Finally, when $t < 0$ we adopt the convention that $I_{\leq t}[z] = I_{\leq t}^{\sigma, \alpha}[z] = \{0\}$.

We will first consider the case when $\alpha = 1$ and $\sigma(x) = x + b$.

Lemma 2 Let \mathbb{F} be a field of characteristic p . Let b be a non zero element of \mathbb{F} and denote by σ the shift $\sigma : x \mapsto x + b$. Denote by S the mapping defined by:

$$\begin{aligned} S : \mathbb{F}[z] &\rightarrow \mathbb{F}[z] \\ P(z) &\mapsto \sum_{i=0}^{p-1} P(\sigma^i(z)) \end{aligned}$$

We have for every nonnegative integer t :

$$\begin{aligned} S(\mathbb{F}_{\leq t}[z]) &= I_{\leq \lfloor \frac{t-p+1}{p} \rfloor_p}^{\sigma}[z] \\ &= \left\{ P(z^p - b^{p-1}z) \mid \deg P \leq \left\lfloor \frac{t-p+1}{p} \right\rfloor \right\} \end{aligned} \quad (4)$$

The proof of this lemma can be found in Appendix B. A similar result holds for affine maps of the form $\sigma(x) = ax + b$ where $a \neq 1$.

Lemma 3 Let \mathbb{F} be a finite field. Let a be an element of order $\ell \neq 1$ in \mathbb{F} , b be an arbitrary element of \mathbb{F} , σ be the affine map $x \mapsto ax + b$, d be an integer in the range $[0, \dots, \ell - 1]$ and let $\alpha \stackrel{\text{def}}{=} a^d$. We define S by

$$\begin{aligned} S : \mathbb{F}[z] &\rightarrow \mathbb{F}[z] \\ P(z) &\mapsto \sum_{i=0}^{\ell-1} \alpha^i P(\sigma^i(z)) \end{aligned}$$

If we denote by z_0 the unique fixed point of σ , we have:

$$S(\mathbb{F}_{\leq t}[z]) = I_{\leq t}^{\sigma, \alpha}[z] \quad (5)$$

$$= \left\{ (z - z_0)^d P((z - z_0)^\ell) \mid \deg P \leq \left\lfloor \frac{t - \ell + d}{\ell} \right\rfloor \right\}, \quad (6)$$

The proof of this lemma can be found in Subsection C of the appendix.

V. REDUCING TO A SMALLER ALTERNANT OR GOPPA CODE

A. Folded codes

Alternant codes and Goppa codes in particular with a certain non-trivial automorphism group (as considered in Proposition 3) meet a very peculiar property. Namely it is possible to derive a new alternant (or a Goppa code) with smaller parameters by simply summing up the coordinates. To define this new code more precisely, we introduce the following operator.

Definition 5 (Folded code) Let \mathcal{C} be a code and \mathbb{G} be a subgroup of permutations of the set of code positions of \mathcal{C} . For each orbit $\mathbb{G}(i) \stackrel{\text{def}}{=} \{\sigma(i) : \sigma \in \mathbb{G}\}$ we choose one representative (for instance the smallest one). Let i_0, i_1, \dots, i_{s-1} be the set of these representatives. The folded code of \mathcal{C} with respect to \mathbb{G} , denoted by $\overline{\mathcal{C}}^{\mathbb{G}}$, is a code of length s which is given by the set of words $\overline{\mathbf{c}}^{\mathbb{G}} \stackrel{\text{def}}{=} (\sum_{\sigma \in \mathbb{G}} c_{\sigma(i_j)})_{0 \leq j \leq s-1}$, where \mathbf{c} ranges over \mathcal{C} . When \mathbb{G} is generated by a single element σ , that is $\mathbb{G} = \langle \sigma \rangle$, we will simply write $\overline{\mathcal{C}}^{\sigma}$ instead of $\overline{\mathcal{C}}^{\langle \sigma \rangle}$ and $\overline{\mathbf{c}}^{\sigma}$ instead of $\overline{\mathbf{c}}^{\langle \sigma \rangle}$.

This folded code is related to constructions which were considered in the framework of decoding codes with non-trivial automorphism group [24], [25]. The approach there was to consider for a code \mathcal{C} with non-trivial permutation automorphism σ of order ℓ (which was supposed to be of order $\ell = 2$ in [24], [25], but their approach generalizes easily to other orders) the σ -subcode $\tilde{\mathcal{C}}^{\sigma}$ obtained as follows:

$$\tilde{\mathcal{C}}^{\sigma} \stackrel{\text{def}}{=} \left\{ \mathbf{c} + \mathbf{c}^{\sigma} + \dots + \mathbf{c}^{\sigma^{\ell-1}} \mid \mathbf{c} \in \mathcal{C} \right\}.$$

If we denote by $\tilde{\mathbf{c}}^{\sigma} \stackrel{\text{def}}{=} \mathbf{c} + \mathbf{c}^{\sigma} + \dots + \mathbf{c}^{\sigma^{\ell-1}}$ then it turns out that $\tilde{\mathbf{c}}^{\sigma}$ takes on a constant value on the orbit $i, \sigma(i), \sigma^2(i), \dots$ of any code position i that is precisely the term $\sum_{t=0}^{\ell-1} c_{\sigma^t(i)}$ which appears in the definition of the folded code. Stated differently, the words of $\tilde{\mathcal{C}}^{\sigma}$ are nothing but the words of $\overline{\mathcal{C}}^{\sigma}$ where each code coordinate \tilde{c}_i^{σ} of the latter code is repeated as many times as the size of the orbit of i under σ . These two codes have therefore the same dimension, but their lengths are different : the first one has the same length as \mathcal{C} whereas the latter has length s (the number of orbits under σ).

The point of considering such a code for decoding \mathcal{C} lies in the fact that $\tilde{\mathcal{C}}^{\sigma}$ is a subcode of \mathcal{C} which is typically of much smaller dimension than \mathcal{C} . Under mild assumptions, it can be shown that the dimension gets reduced by the order of σ . More precisely:

Proposition 6 Let \mathcal{C} be a code of length n that has a permutation automorphism group \mathbb{G} of size ℓ and a generator matrix \mathbf{G} such that if \mathbf{g}_i is a row of \mathbf{G} then \mathbf{g}_i^{σ} is also a row of \mathbf{G} for any $\sigma \in \mathbb{G}$. Denote by $\{\mathbf{g}_0, \dots, \mathbf{g}_{k-1}\}$ the set of rows of \mathbf{G} . Consider the group action of \mathbb{G} on the set $\{\mathbf{g}_0, \dots, \mathbf{g}_{k-1}\}$ of rows of \mathbf{G} where σ acts on \mathbf{g}_j as $\mathbf{g}_j \mapsto \mathbf{g}_j^{\sigma}$ for $\sigma \in \mathbb{G}$. Assume that the size of each orbit is equal to ℓ . Then, the dimension of $\tilde{\mathcal{C}}^{\mathbb{G}}$ is equal to $\frac{\dim(\mathcal{C})}{\ell}$. This is also the dimension of $\overline{\mathcal{C}}^{\mathbb{G}}$ and the length of this code is equal to $\frac{n}{\ell}$.

Proof: This follows at once from the fact that $\tilde{\mathcal{C}}^{\mathbb{G}}$ is generated by the set of $\tilde{\mathbf{g}}_i^{\mathbb{G}} \stackrel{\text{def}}{=} \sum_{\sigma \in \mathbb{G}} \mathbf{g}_i^{\sigma}$ where the \mathbf{g}_i 's are representatives of each orbit of \mathbb{G} acting on $\{\mathbf{g}_0, \dots, \mathbf{g}_{k-1}\}$. These vectors are clearly independent and there are $\frac{\dim(\mathcal{C})}{\ell}$ such representatives. This implies that the dimension of $\tilde{\mathcal{C}}^{\mathbb{G}}$ is equal to $\frac{\dim(\mathcal{C})}{\ell}$. This is also clearly the dimension of $\overline{\mathcal{C}}^{\mathbb{G}}$ and the length of the latter code is equal to $\frac{n}{\ell}$. ■

Remark 3 A generator matrix of this form is precisely what is achieved by all the constructions of monoidic alternant/Goppa/Srivastava codes proposed in [4], [5], [1], [13], [6].

This can be used to decode a word \mathbf{y} by decoding instead $\tilde{\mathbf{y}}^{\sigma}$ in $\tilde{\mathcal{C}}^{\sigma}$. The point is that this decoding can be less complex to perform than decoding \mathbf{y} directly and that the result of the decoding can be useful to solve the original decoding problem, see [25].

B. Folding alternant codes with respect to a cyclic group

If we consider the monoidic alternant or Goppa codes constructed in [4], [5], [1], [13] they have typically length of the form $n = n_0\ell$, degree of the form $r = r_0\ell$ and dimension of the form $k = n - rm = \ell(n_0 - r_0m)$ where m is the extension degree of the alternant/Goppa code and ℓ is the size of the automorphism group of the code. The automorphism group of these codes satisfies the assumptions of Proposition 6 and therefore the folded code has length n_0 and dimension $n_0 - r_0m$. This could suggest that these codes are alternant or Goppa codes of length n_0 and degree r_0 . In all our experiments we have noticed that this was indeed the case. We have proved in [21] a slightly weaker result, namely that in the case of a Goppa code obtained from the constructions of [5], [1], [13], the folded code is included in a Goppa code of length n_0 and degree r_0 . We will prove a significantly stronger result here, by considering instead the dual of these codes. It will turn out that the folded dual of those alternant or Goppa codes will be duals of alternant or Goppa codes and this even if the degree is not of the form $r_0\ell$. More precisely, we have:

Theorem 1 Consider an alternant code $\mathcal{A}_t(\mathbf{x}, \mathbf{y})$ over \mathbb{F}_q of length n with support $\mathbf{x} = (x_0, x_1, \dots, x_{n-1}) \in \mathbb{F}_{q^m}^n$ and multiplier $\mathbf{y} \in \mathbb{F}_{q^m}^n$ with a non trivial permutation automorphism group induced by the affine map $x \rightarrow ax + b$ where $a, b \in \mathbb{F}_{q^m}$ are such that $a \neq 0$ and $b \neq 0$ when $a = 1$. Denote by σ the permutation of S_n induced by this affine map. Let ℓ be the order of σ . By definition of an affine induced automorphism, there exists $\alpha \in \mathbb{F}_{q^m}$ an ℓ -th root of unity such that $y_{\sigma(i)} = \alpha y_i$ for all $i \in \{0, 1, \dots, n-1\}$. We denote by d the integer in $\{0, 1, \dots, \ell-1\}$ verifying $\alpha = a^d$. Let us denote by u_0 the unique fixed point in $\mathbb{F}_{q^m} \cup \{\infty\}$ of this affine map. Moreover, we assume that $u_0 \notin \{x_0, x_1, \dots, x_{n-1}\}$. In such a case, the action of σ on $\{0, 1, \dots, n-1\}$ has $\frac{n}{\ell}$ orbits, each of them being of size ℓ . Choose a representative $i_0, i_1, \dots, i_{n/\ell-1}$ in each of these orbits. There exists $\mathbf{y}' \in \mathbb{F}_{q^m}^{n/\ell}$ and a integer r such that $\overline{(\mathcal{A}_t(\mathbf{x}, \mathbf{y})^\perp)^\sigma} = (\mathcal{A}_r(\mathbf{x}', \mathbf{y}'))^\perp$ with:

- when $a = 1$ then $r = \lfloor \frac{t-\ell}{\ell} \rfloor + 1$ and for all $j \in \{0, \dots, n/\ell - 1\}$:

$$x'_j = x_{i_j}^\ell - b^{\ell-1}x_{i_j} \quad \text{and} \quad y'_j = y_{i_j}$$

- and when $a \neq 1$ then $r = \lfloor \frac{t-\ell+d-1}{\ell} \rfloor + 1$ and for all $j \in \{0, \dots, n/\ell - 1\}$:

$$x'_j = (x_{i_j} - u_0)^\ell \quad \text{and} \quad y'_j = y_{i_j}(x_{i_j} - u_0)^{\ell-d}$$

Proof:

The case $a = 1$: remark first that the order ℓ of the permutation σ , which is the shift $x \mapsto x + b$ in this case, is necessarily the characteristic p of \mathbb{F}_{q^m} . Since the order of the multiplicative group of \mathbb{F}_{q^m} , which is $q^m - 1$, is coprime with the characteristic of \mathbb{F}_{q^m} it follows that α is necessarily equal to 1 when $a = 1$. This implies that \mathbf{y} is constant over each orbit $\{i, \sigma(i), \dots, \sigma^{\ell-1}(i)\}$. From Lemma 1, the dual \mathcal{C} of $\mathcal{A}_t(\mathbf{x}, \mathbf{y})$ is:

$$\mathcal{C} = \left\{ (\text{Tr}(y_i P(x_i)))_{0 \leq i < n} \mid P \in \mathbb{F}_{q^m}[z], \deg P \leq t-1 \right\}.$$

The folded code of \mathcal{C} can now be described as:

$$\overline{\mathcal{C}^\sigma} = \left\{ \text{Tr} \left(y_{i_j} \sum_{s=0}^{\ell-1} P(\sigma^s(x_{i_j})) \right)_{j=0}^{n/\ell-1} \mid P \in \mathbb{F}_{q^m}[z], \deg P \leq t-1 \right\}$$

where $x_{i_0}, x_{i_1}, \dots, x_{i_{n/\ell-1}}$ are representatives of each of the n/ℓ orbits $\{u, \sigma(u), \dots, \sigma^{\ell-1}(u)\}$ (they have all the same size ℓ).

By using Lemma 2, we obtain:

$$\overline{\mathcal{C}^\sigma} = \left\{ \text{Tr} \left(y_{i_j} R \left(x_{i_j}^p - b^{p-1}x_{i_j} \right) \right)_{j=0}^{n/\ell-1} \mid R \in \mathbb{F}_{q^m}[z], \deg R \leq \left\lfloor \frac{t-p}{p} \right\rfloor \right\} \quad (7)$$

By using Lemma 1 again, we see that $\overline{\mathcal{C}^\sigma} = \mathcal{A}_r(\mathbf{x}', \mathbf{y}')^\perp$ with $r = \left\lfloor \frac{t-p}{p} \right\rfloor + 1$ and for any $j \in \{0, 1, \dots, n/\ell - 1\}$, $x'_j = x_{i_j}^p - b^{p-1}x_{i_j}$ and $y'_j = y_{i_j}$.

The case $a \neq 1$: the difference with the previous situation lies in the fact that now the y_j 's are not necessarily constant over an orbit. As previously, we consider representatives $x_{i_0}, x_{i_1}, \dots, x_{n/\ell-1}$ of the n/ℓ orbits $\{u, \sigma(u), \dots, \sigma^{\ell-1}(u)\}$ (they have here again all the same size ℓ because the support \mathbf{x} does not contain the fixed point of σ). We obtain that the folded code of \mathcal{C} can now be described as follows.

$$\overline{\mathcal{C}^\sigma} = \left\{ \text{Tr} \left(\sum_{s=0}^{\ell-1} y_{i_j} \alpha^s P(\sigma^s(x_{i_j})) \right) \right\}_{j=0}^{n/\ell-1} \mid P \in \mathbb{F}_{q^m}[z], \deg P \leq t-1 \right\}.$$

By introducing the fixed point u_0 of σ , we obtain:

$$\begin{aligned} \overline{\mathcal{C}^\sigma} &= \left\{ \text{Tr} \left(y_{i_j} \sum_{s=0}^{\ell-1} \alpha^s P(u_0 + a^s(x_{i_j} - u_0)) \right) \right\}_{j=0}^{n/\ell-1} \mid P \in \mathbb{F}_{q^m}[z], \deg P \leq t-1 \right\} \\ &= \left\{ \text{Tr} \left(y_{i_j} \sum_{s=0}^{\ell-1} \alpha^s Q(a^s(x_{i_j} - u_0)) \right) \right\}_{j=0}^{n/\ell-1} \mid Q \in \mathbb{F}_{q^m}[z], \deg Q \leq t-1 \right\}. \end{aligned}$$

We necessarily have $\alpha^\ell = 1$. Since a is a primitive ℓ -root of unity, there exists an integer d in $\{0, \dots, \ell-1\}$ such that $\alpha = a^d$. This yields:

$$\overline{\mathcal{C}^\sigma} = \left\{ \text{Tr} \left(y_{i_j} \sum_{s=0}^{\ell-1} a^{ds} Q(a^s(x_{i_j} - u_0)) \right) \right\}_{j=0}^{n/\ell-1} \mid Q \in \mathbb{F}_{q^m}[z], \deg Q \leq t-1 \right\}.$$

By using Lemma 3, we deduce that:

$$\overline{\mathcal{C}^\sigma} = \left\{ \text{Tr} \left(y_{i_j} (x_{i_j} - u_0)^{\ell-d} R((x_{i_j} - u_0)^\ell) \right) \right\}_{j=0}^{n/\ell-1} \mid R \in \mathbb{F}_{q^m}[z], \deg R \leq \left\lfloor \frac{t-1-\ell+d}{\ell} \right\rfloor \right\}.$$

Finally, by Lemma 1 again we see that $\overline{\mathcal{C}^\sigma} = \mathcal{A}_r(\mathbf{x}', \mathbf{y}')^\perp$ where $r = \left\lfloor \frac{t-1-\ell+d}{\ell} \right\rfloor + 1$, $x'_j = (x_{i_j} - u_0)^\ell$ and $y'_j = y_{i_j} (x_{i_j} - u_0)^{\ell-d}$ for any $j \in \{0, 1, \dots, n/\ell-1\}$. ■

Remark 4 In essence, we have proved here that folding a GRS code with a non trivial automorphism group obtained from affine transformations yields again a GRS code. Indeed, the dual of an alternant code is the trace of a GRS code. When we choose the extension degree to be equal to 1 we really prove here that folding such a symmetric GRS code yields again a GRS code. Taking the trace preserves this property : the folding of a trace of a symmetric GRS code is again the trace of a GRS code. The crucial point which explains why such a property holds is the fact that the ring of polynomial in $\mathbb{F}[x]$ invariant by an affine transformation σ is a ring of the form $\mathbb{F}[Q(x)]$ for some polynomial Q which is invariant by σ . This is what allows to write a sum of the form $\sum_{i=0}^{\ell-1} P(\sigma^i(x))$ as a polynomial of the form $R(Q(x))$.

One might wonder whether folding a subfield subcode of a GRS code (i.e. an alternant code) also yields a subfield subcode of a GRS code. While the proof technique used here obviously allows to prove that a folded subfield subcode of a symmetric GRS code lies in a subfield subcode of a certain subcode, proving equality of both codes seems to be more delicate here. This point can be explained as follows. Consider an alternant code $\mathcal{A}_r(\mathbf{x}, \mathbf{y})$ defined over \mathbb{F}_q and of extension degree m where \mathbf{x} is globally invariant by some σ and \mathbf{y} is constant on the orbits on σ (we make this assumption to simplify the discussion). To prove equality that the folded alternant code is still an alternant code we should be able to express a polynomial $Q(z)$ in $\mathbb{F}_{q^m}[z]$ which is invariant by σ and which is such that $y_i Q(x_i)$ belongs to \mathbb{F}_q for any i as a sum $Q(x) = \sum_{j=0}^{\ell-1} P(\sigma^j(x))$ where all the $y_i P(\sigma^j(x_i))$ belong to \mathbb{F}_q for any i and j and where P is some polynomial which depends on Q .

C. Folding alternant codes with respect to non-cyclic groups

We have treated the case of folding an alternant code with respect to a group generated by a single element. The group of automorphism might not be cyclic. This happens in particular in the case of the Goppa codes in [5], [1], [13]: in such a case the automorphism group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\lambda$. Treating the general case of a subgroup of the affine subgroup is beyond the scope of this article, we will just consider the case of a subgroup which is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\lambda$. This follows at once from Theorem 1 by noticing that we may fold iteratively the code with respect to λ generators of the subgroup and end up with an alternant code. We use here the straightforward fact

Lemma 4 *Consider a code \mathcal{C} and a group of permutations \mathbb{G} acting on the positions of \mathcal{C} and assume that this permutation group has a subgroup \mathbb{G}_0 and an element σ of \mathbb{G} which does not belong to \mathbb{G}_0 such that:*

- 1) *the cosets $\sigma^i \mathbb{G}_0$ form a partition of \mathbb{G} for $i \in \{0, \dots, \ell - 1\}$ where ℓ is the order of σ ;*
- 2) *σ commutes with any element of \mathbb{G}_0 .*

Then σ induces a permutation on the set of positions of $\overline{\mathcal{C}^{\mathbb{G}_0}}$ that we call $\hat{\sigma}$ which is defined as follows. We view a code position i of $\overline{\mathcal{C}^{\mathbb{G}_0}}$ as an orbit $\{\tau(u), \tau \in \mathbb{G}_0\}$ for some code position u of \mathcal{C} and $\hat{\sigma}(i)$ is given by the orbit $\{\tau(\sigma(u)), \tau \in \mathbb{G}_0\}$. If the order of $\hat{\sigma}$ is equal to the order ℓ of σ and for an appropriate order on the choices of the representatives for the orbits under $< \hat{\sigma} >$, \mathbb{G}_0 and \mathbb{G} , we have

$$\overline{(\overline{\mathcal{C}^{\mathbb{G}_0}})^{\hat{\sigma}}} = \overline{\mathcal{C}^{\mathbb{G}}}.$$

Proof: First we have to check that the definition of $\hat{\sigma}(u)$ makes sense, i.e. that it does not depend on the choice of u in the orbit $\{\tau(u), \tau \in \mathbb{G}_0\}$. This follows from the fact that σ commutes with any element of \mathbb{G}_0 . Indeed assume that we have:

$$\{\tau(u), \tau \in \mathbb{G}_0\} = \{\tau(v), \tau \in \mathbb{G}_0\}$$

then we clearly have $u = \tau_0(v)$ for a certain τ_0 in \mathbb{G}_0 . From that we deduce:

$$\begin{aligned} \{\tau(\sigma(u)), \tau \in \mathbb{G}_0\} &= \{\tau(\sigma(\tau_0(v))), \tau \in \mathbb{G}_0\} \\ &= \{\tau(\tau_0(\sigma(v))), \tau \in \mathbb{G}_0\} \\ &= \{\tau(\sigma(v)), \tau \in \mathbb{G}_0\} \end{aligned}$$

This shows that $\hat{\sigma}$ is well-defined. We let i_0, i_1, \dots, i_{s-1} be a set of representatives of each orbit of the code positions of \mathcal{C} under \mathbb{G}_0 (we assume that there are s orbits) and we assume that the set of code positions $0, 1, \dots, s-1$ of $\overline{\mathcal{C}^{\mathbb{G}_0}}$ corresponds to i_0, i_1, \dots, i_{s-1} in this order. Consider now an element c in \mathcal{C} and let c' be the folding of c with respect to \mathbb{G}_0 , that is:

$$c'_j = \sum_{\tau \in \mathbb{G}_0} c_{\tau(i_j)} \quad (8)$$

If we fold c' with respect to $\hat{\sigma}$ we obtain an element c'' defined by:

$$c''_j = \sum_{l=0}^{\ell-1} c'_{\hat{\sigma}^l(i'_j)} \quad (9)$$

where $i'_0, i'_1, \dots, i'_{t-1}$ are the representatives of the orbits of the code positions of $\overline{\mathcal{C}^{\mathbb{G}_0}}$ under $\hat{\sigma}$. Notice that we have used here the fact that the order of $\hat{\sigma}$ is equal to the order of σ . By observing that the code position i'_j of $\overline{\mathcal{C}^{\mathbb{G}_0}}$ corresponds to some orbit $\{\tau(u), \tau \in \mathbb{G}_0\}$ and putting (8) and (9) together with the characterization of the action of $\hat{\sigma}$, we obtain:

$$c''_j = \sum_{l=0}^{\ell-1} \sum_{\tau \in \mathbb{G}_0} c_{\tau(\sigma^l(u))} = \sum_{\tau \in \mathbb{G}} c_{\tau(u)}.$$

This implies that c''_j is equal to some coordinate of $\overline{\mathcal{C}^{\mathbb{G}}}$.

It remains to show that there is a one-to-one and onto mapping from the set of coordinates of \mathcal{C}'' and those of $\overline{\mathcal{C}^{\mathbb{G}}}$. In order to do so we are going to prove that there is a one-to-one mapping between the orbits under $\hat{\sigma}$ and the orbits under \mathbb{G} . This is a straightforward consequence of the following observation. Consider an orbit $\mathcal{O} = \{\tau(s), \tau \in \mathbb{G}\}$ under \mathbb{G} . It decomposes as a union of orbits \mathcal{O}_h under \mathbb{G}_0 : $\mathcal{O} = \bigcup_{0 \leq h \leq \ell-1} \mathcal{O}_h$ where $\mathcal{O}_h \stackrel{\text{def}}{=} \{\tau(\sigma^h(s))\}$. These orbits \mathcal{O}_h form a single orbit under $\hat{\sigma}$ and we are done. ■

A straightforward consequence of this is the following

Corollary 2 *Consider a code \mathcal{C} which is the dual of an alternant code with an affine-induced permutation group \mathbb{G} isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\lambda$ where p is the characteristic of the field over which the alternant code is defined. Then $\overline{\mathcal{C}^{\mathbb{G}}}$ is the dual of an alternant code.*

Proof: In such a case, there exists g_1, \dots, g_λ of order p that generate \mathbb{G} . We proceed by induction and assume that this property holds for $\lambda = h$. When $h = 1$, this is just Theorem 1. Consider now a group \mathbb{G} isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{h+1}$. We observe that $\mathbb{G}_0 \stackrel{\text{def}}{=} \langle g_1, \dots, g_h \rangle$ and $\sigma = g_{h+1}$ satisfy the assumptions of Lemma 4, so we can apply it to this case and obtain that:

$$\overline{(\overline{\mathcal{C}^{\mathbb{G}_0}})^{\hat{\sigma}}} = \overline{\mathcal{C}^{\mathbb{G}}}.$$

Since by induction hypothesis $\overline{\mathcal{C}^{\mathbb{G}_0}}$ is the dual of an alternant code and since $\hat{\sigma}$ is clearly an affine induced permutation automorphism of $\overline{\mathcal{C}^{\mathbb{G}_0}}$ we can apply Theorem 1 to it and obtain that the result of the folding of $\overline{\mathcal{C}^{\mathbb{G}_0}}$ by $\hat{\sigma}$ gives an alternant code again. ■

All the duals of the codes used in the following variants of the McEliece cryptosystem, namely the dyadic Goppa codes of [5], [13], the monoidic Goppa codes of [1] or the dyadic Srivastava codes of [6] are instances of alternant codes which have an affine induced permutation group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\lambda$ and this corollary can be applied to reduce attacks on the key to a much smaller key recovery problem (namely on the dual of the code obtained by folding). One might also wonder when we fold certain subfamilies of duals of alternant codes with respect to an affine-induced permutation automorphism group, such as duals of Goppa codes, we stay in the subfamily, i.e. *do we still obtain the dual of a Goppa code?* This turns out to be the case as shown by the next subsection.

D. Folding Goppa codes

Folding the dual of a Goppa code with an affine-induced automorphism group yields the dual of an alternant code by using Corollary 2. It turns out that a stronger statement holds: we actually obtain the dual of a Goppa code, both in the cyclic case as shown by the following theorem and when the group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\lambda$ as shown later on.

Theorem 2 *Consider a Goppa code $\mathcal{C} = \mathcal{G}(\mathbf{x}, \Gamma(z))$ of length n associated to the support $\mathbf{x} = (x_i)_{0 \leq i < n} \in \mathbb{F}_{q^m}^n$ which has a cyclic affine induced automorphism group generated by $\sigma(x) \stackrel{\text{def}}{=} ax + b$ where $a, b \in \mathbb{F}_{q^m}$. We assume that $a \neq 0$, $b \neq 0$ if $a = 1$, and that the fixed point u_0 of σ does not belong to $\{x_0, \dots, x_{n-1}\}$. Let ℓ be the order of σ . In such a case:*

- 1) ℓ divides n and let $s \stackrel{\text{def}}{=} n/\ell$. There are exactly s orbits for the action of σ on the code positions. We denote by i_0, i_1, \dots, i_{s-1} a set of representatives for each orbit;
- 2) $(\mathcal{C}^\perp)^\sigma$ is the dual of the Goppa code $\mathcal{G}(\mathbf{x}', \gamma(z))$ with:

$$\begin{aligned} x'_j &= \begin{cases} x_{i_j}^\ell - b^{\ell-1}x_{i_j} & \text{when } a = 1, \\ (x_{i_j} - u_0)^\ell & \text{otherwise,} \end{cases} \\ \Gamma(z) &= \begin{cases} \gamma(z^\ell - b^{\ell-1}z) & \text{when } a = 1, \\ (z - u_0)^d \gamma((z - u_0)^\ell) & \text{otherwise} \end{cases} \end{aligned}$$

where d , in the last case, is the unique integer in $\{0, \dots, \ell - 1\}$ such that $\alpha = a^d$ and α is the element of \mathbb{F}_{q^m} which satisfies the polynomial identity $\Gamma(az + b) = \alpha\Gamma(z)$.

Proof: We will distinguish between $a = 1$ and $a \neq 1$. In both cases, notice that we can apply Theorem 1 to \mathcal{C} which is an alternant code $\mathcal{A}_t(\mathbf{x}, \mathbf{y})$ where t is the degree of Γ and $y_i = \frac{1}{\Gamma(x_i)}$. This is a consequence of the definition of a Goppa code with an affine induced automorphism $\sigma(x) = ax + b$: this is a Goppa code obtained from the construction of Proposition 3 and this is precisely what is needed (together with the fact that the support does not contain the fixed point of σ) for applying Theorem 1 to it. In all cases, folding the dual of \mathcal{C} gives the dual of an alternant code of the form $\mathcal{A}_{t'}(\mathbf{x}', \mathbf{y}')$ for some integer t' and some \mathbf{x}', \mathbf{y}' in $\mathbb{F}_{q^m}^s$. Moreover in both cases, there exists an ℓ -th root of 1 that we denote by α which is such that the Goppa polynomial satisfies the identity $\Gamma(az + b) = \alpha\Gamma(z)$.

Case $a = 1$: ℓ is equal to the characteristic p of the field \mathbb{F}_{q^m} , α is necessarily equal to 1, $\Gamma(z)$ is of degree a multiple of p and is of the form $\Gamma(z) = \gamma(z^p - b^{p-1}z)$. Notice that \mathbf{y} satisfies:

$$y_{\sigma(i)} = \frac{1}{\Gamma(ax_i + b)} = \frac{1}{\Gamma(x_i)} = y_i$$

and using Theorem 1 gives that $y'_j = y_{i_j}$ and therefore:

$$y'_j = y_{i_j} = \frac{1}{\Gamma(x_{i_j})} = \frac{1}{\gamma(x_{i_j}^p - b^{p-1}x_{i_j})} = \frac{1}{\gamma(x'_j)}$$

This implies that $\mathcal{A}_{t'}(\mathbf{x}', \mathbf{y}')$ is nothing but the Goppa code $\mathcal{G}(\mathbf{x}', \gamma(z))$.

Case $a \neq 1$: there exists a unique integer d in the range $[0, \dots, \ell - 1]$ such that $\alpha = a^d$ and $\Gamma(z)$ is of the form $\Gamma(z) = (z - u_0)^d \gamma((z - u_0)^\ell)$. Notice that in such a case:

$$\begin{aligned} \frac{1}{y_{\sigma(i)}} &= \Gamma(ax_i + b) = (ax_i + b - u_0)^d \gamma((ax_i - u_0)^\ell) \\ &= (ax_i + b - au_0 - b)^d \gamma((ax_i + b - au_0 - b)^\ell) \\ &= (a(x_i - u_0))^d \gamma(a^\ell (x_i - u_0)^\ell) \\ &= a^d (x_i - u_0)^d \gamma((x_i - u_0)^\ell) \\ &= a^d \Gamma(x_i) = a^d \frac{1}{y_i} \end{aligned}$$

We use Theorem 1 and obtain:

$$y'_j = y_{i_j} (x_{i_j} - u_0)^d = \frac{(x_{i_j} - u_0)^d}{\Gamma(x_{i_j})} = \frac{(x_{i_j} - u_0)^d}{(x_{i_j} - u_0)^d \gamma((x_{i_j} - u_0)^\ell)} = \frac{1}{\gamma(x'_j)}$$

This implies again that $\mathcal{A}_{t'}(\mathbf{x}', \mathbf{y}')$ is nothing but the Goppa code $\mathcal{G}(\mathbf{x}', \gamma(z))$. ■

When the group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\lambda$ we have the following statement

Theorem 3 Consider a Goppa code $\mathcal{C} = \mathcal{G}(\mathbf{x}, \Gamma)$ with an affine induced automorphism group \mathbb{G} isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\lambda$ where p is the characteristic of the field over which the Goppa code is defined, then the folding $(\mathcal{C}^\perp)^\mathbb{G}$ is the dual of a Goppa code $\mathcal{G}(\mathbf{x}', \gamma(z))$ where the degree $\deg(\gamma)$ of γ is equal to $\frac{\deg(\Gamma)}{p^\lambda}$.

Proof: We proceed similarly to the proof of Corollary 2. First we notice that there exists g_1, \dots, g_λ of order p that generate \mathbb{G} . We proceed by induction and assume that this property holds for $\lambda = h$. When $h = 1$, this is just Theorem 2 (since g_1 is necessarily induced by an affine transformation of the form $x \mapsto x + \beta$ which has no fixed point in the extension field in which the coordinates of the multiplier live). Consider now a group \mathbb{G} isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{h+1}$. We observe that $\mathbb{G}_0 \stackrel{\text{def}}{=} \langle g_1, \dots, g_h \rangle$ and $\sigma = g_{h+1}$ satisfy the assumptions of Lemma 4, so we can apply it to this case and obtain that:

$$\overline{(\mathcal{C}^{\mathbb{G}_0})^\sigma} = \mathcal{C}^\mathbb{G}.$$

Since by induction hypothesis $\overline{\mathcal{C}^{\mathbb{G}_0}}$ is the dual of a Goppa code of degree $\frac{\deg(\Gamma)}{p^h}$ and since $\hat{\sigma}$ is clearly an affine induced permutation automorphism of $\overline{\mathcal{C}^{\mathbb{G}_0}}$ we can apply Theorem 2 to it and obtain that the result of the folding of $\overline{\mathcal{C}^{\mathbb{G}_0}}$ by $\hat{\sigma}$ gives the dual of a Goppa code of degree $\frac{\deg(\Gamma)}{p^{h+1}}$. ■

VI. CONCLUSION – CRYPTOGRAPHIC IMPLICATIONS

The results presented on this paper have some significant consequences on a recent research trend which consists in devising McEliece schemes with reduced public key size. This is achieved by relying on QD/QM Goppa codes or QC alternant codes [4], [5], [13], [1]. Some of them were attacked by the algebraic attack introduced in [9], [11] where it was proved that the QD or the QC structure allowed to set up an algebraic system which could be solved by Gröbner bases techniques thanks to the reduction of unknowns obtained in this case compared to an unstructured McEliece scheme. Our result actually explains where this reduction in the number of unknowns comes from: there is in fact a smaller *hidden* Goppa (or alternant) code behind the public generator or parity-check matrix of the scheme. Moreover it is shown in [21] that a key recovery attack on the reduced cryptosystem can be used to recover the secret key of the original cryptosystem. This implies that a key-recovery on QD and QM schemes is not harder than a key-recovery on a reduced McEliece scheme where all parameters have been scaled down by a factor of p , which is the compression factor allowed by the QC, QD or QM structure. For instance, we can reduce the key-recovery of a QD Goppa code of length 8192 and dimension 4096 (parameters suggested in [5]) to the key-recovery on a QD Goppa code of length 64 and dimension 32. In other words, the very reason which allowed to design compact variants of McEliece can be used to attack such schemes much more efficiently.

Our result does not rule out the possibility of devising alternant or Goppa codes with a non trivial automorphism group for which folding does not produce an alternant or a Goppa code: it only applies to such codes with an affine induced automorphism group. Symmetric codes of this kind could be obtained from the action of the semi-linear projective group on the support instead of the affine group (see Section III). It is an open question to understand if folding such symmetric codes yields again Goppa or alternant codes, but obviously even treating the case of the linear projective group (obtained from the transformations of the kind $z \rightarrow \frac{az+b}{cz+d}$) needs much more general tools than those that have been considered here and is beyond the scope of this paper. It should also be added that this result does not mean that all compact key McEliece cryptosystems based on alternant or Goppa codes with an affine induced automorphism group are weak. It just means that the key security is not better than the key security of a reduced scheme obtained from the folding process. Since key recovery attacks are generally more expensive than message recovery attacks it might be possible to choose secure parameters for which we still obtain a good reduction of the key size where key recovery attacks on the folded key are of the same complexity as message recovery attacks on the original scheme. However this thread of research requires great care since there has been some recent progress on key recovery attacks, see [21], [26] for instance.

REFERENCES

- [1] P. S. L. M. Barreto, R. Lindner, and R. Misoczki, “Monoidic codes in cryptography,” in *PQCrypto*, ser. Lecture Notes in Computer Science, B.-Y. Yang, Ed., vol. 7071. Springer, 2011, pp. 179–199.
- [2] R. Misoczki, J.-P. Tillich, N. Sendrier, and P. S. L. M. Barreto, “MDPC-McEliece: New McEliece variants from moderate density parity-check codes,” in *ISIT*, 2013, pp. 2069–2073.
- [3] P. Gaborit, “Shorter keys for code based cryptography,” in *Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)*, Bergen, Norway, Mar. 2005, pp. 81–91.
- [4] T. P. Berger, P. Cayrel, P. Gaborit, and A. Otmani, “Reducing key length of the McEliece cryptosystem,” in *Progress in Cryptology - Second International Conference on Cryptology in Africa (AFRICACRYPT 2009)*, ser. Lecture Notes in Computer Science, B. Preneel, Ed., vol. 5580, Gammarth, Tunisia, Jun. 21–25 2009, pp. 77–97.
- [5] R. Misoczki and P. S. L. M. Barreto, “Compact McEliece keys from Goppa codes,” in *Selected Areas in Cryptography (SAC 2009)*, Calgary, Canada, Aug. 13–14 2009.
- [6] E. Persichetti, “Compact McEliece keys based on quasi-dyadic Srivastava codes,” *J. Mathematical Cryptology*, vol. 6, no. 2, pp. 149–169, 2012.
- [7] A. Otmani, J. Tillich, and L. Dallot, “Cryptanalysis of McEliece cryptosystem based on quasi-cyclic LDPC codes,” in *Proceedings of First International Conference on Symbolic Computation and Cryptography*. Beijing, China: LMIB Beihang University, Apr. 28–30 2008, pp. 69–81.

- [8] —, “Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes,” *Mathematics in Computer Science*, vol. 3, no. 2, pp. 129–140, 2010.
- [9] J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich, “Algebraic cryptanalysis of McEliece variants with compact keys,” in *EUROCRYPT*, 2010, pp. 279–298.
- [10] —, “Algebraic Cryptanalysis of McEliece variants with compact keys – toward a complexity analysis,” in *SCC '10: Proceedings of the 2nd International Conference on Symbolic Computation and Cryptography*, RHUL, June 2010, pp. 45–55. [Online]. Available: <http://www.polsys.lip6.fr/~jcf/Papers/SCC2010a.pdf>
- [11] V. G. Umana and G. Leander, “Practical key recovery attacks on two McEliece variants,” in *International Conference on Symbolic Computation and Cryptography–SCC*, vol. 2010, 2010, p. 62.
- [12] S. Heyse, “Implementation of McEliece based on quasi-dyadic Goppa codes for embedded devices,” in *Post-Quantum Cryptography*, ser. Lecture Notes in Computer Science, B.-Y. Yang, Ed. Springer Berlin Heidelberg, 2011, vol. 7071, pp. 143–162. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-25405-5_10
- [13] P. S. L. M. Barreto, P.-L. Cayrel, R. Misoczki, and R. Niebuhr, “Quasi-dyadic CFS signatures,” in *Inscrypt*, ser. Lecture Notes in Computer Science, X. Lai, M. Yung, and D. Lin, Eds., vol. 6584. Springer, 2010, pp. 336–349.
- [14] M. Barbier, “Key reduction of McEliece’s cryptosystem using list decoding,” *CoRR*, vol. abs/1102.2566, 2011.
- [15] G. Bommier and F. Blanchet, “Binary quasi-cyclic Goppa codes,” *Designs, Codes and Cryptography*, vol. 20, no. 2, pp. 107–124, 2000.
- [16] J. Ryan and P. Fitzpatrick, “Quasicyclic irreducible Goppa codes,” in *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, June 2004, p. 183.
- [17] T. P. Berger, “Cyclic alternant codes induced by an automorphism of a GRS code,” in *Finite fields: Theory, Applications and Algorithms*, R. Mullin and G. Mullen, Eds., vol. 225. Waterloo, Canada: AMS, Contemporary Mathematics, 1999, pp. 143–154.
- [18] —, “Goppa and related codes invariant under a prescribed permutation,” *IEEE Trans. Inform. Theory*, vol. 46, no. 7, p. 2628, 2000.
- [19] —, “On the cyclicity of Goppa codes, parity-check subcodes of Goppa codes and extended Goppa codes,” *Finite Fields and Applications*, vol. 6, pp. 255–281, 2000.
- [20] A. Dür, “The automorphism groups of Reed-Solomon codes,” *J. Combin. Theory Ser. A*, vol. 44, pp. 69–82, 1987.
- [21] J.-C. Faugère, A. Otmani, L. Perret, F. de Portzamparc, and J.-P. Tillich, “Structural cryptanalysis of McEliece-like schemes with compact keys,” *IACR Cryptology ePrint Archive*, vol. 2014, p. 210, 2014.
- [22] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 5th ed. Amsterdam: North-Holland, 1986.
- [23] P. Delsarte, “On subfield subcodes of modified Reed-Solomon codes,” *IEEE Transactions on Information Theory*, vol. 21, no. 5, pp. 575–576, 1975.
- [24] M. Legeay, “Towards an approach using algebraic properties of the σ -subcode,” in *Proceedings of the Workshop on Coding and Cryptography, WCC 2011*, ed. by D. Augot and A. Canteaut, Eds., Paris, France, 2011, pp. 193–202.
- [25] —, “Utilisation du groupe de permutations d’un code correcteur pour améliorer l’efficacité du décodage,” Ph.D. dissertation, Univ. Rennes 1, 2012.
- [26] A. Couvreur, A. Otmani, and J.-P. Tillich, “Polynomial time attack on wild McEliece over quadratic extensions,” 2014, arXiv:1402.3264. To appear EUROCRYPT 2014.
- [27] I. Shafarevich, *Basic Algebraic Geometry, Varieties in Projective Space*, 2nd ed. Springer Verlag, 1994, vol. Vol. 1.

APPENDIX

A. Proof of Proposition 4

We will first characterize the solutions to Equation (1) in the case where $\alpha = 1$. In some sense, this characterization generalizes a classical result about even polynomials, i.e. polynomials $P(z)$ which satisfy $P(z) = P(-z)$. It is namely well known that a polynomial is even if and only if there exists a polynomial Q such that $P(z) = Q(z^2)$. Lemma 5, which uses the notation $I_{\leq t}^\sigma[z]$ that is defined in Section IV, will generalize this result to any polynomial invariant under a finite order affine map.

Lemma 5 *Let $\sigma(z) = az + b$ be an affine map of finite order ℓ (with $\ell > 1$) defined over a field \mathbb{F} . We have*

- if $a = 1$ then \mathbb{F} is of characteristic ℓ and $I_{\leq t}^\sigma[z] = \{Q(z^\ell - b^{\ell-1}z) \mid \deg Q \leq t/\ell\}$.
- if $a \neq 1$ then $I_{\leq t}^\sigma[z] = \{Q((z - z_0)^\ell) \mid \deg Q \leq t/\ell\}$ with z_0 being the unique fixed point of σ .

In other words, the ring of polynomials invariant by an affine map is generated by a single element and the lemma provides this generator explicitly. This result follows from classical results in invariant theory and we derive it from scratch here to keep the paper self-contained. Also, we treat the case where the order ℓ of the group generated by σ is divisible by the characteristic of \mathbb{F} . This is precisely what happens when $a = 1$, and that is commonly avoided in invariant theory (see for instance [27, Appendix, §4, Prop.1]).

Proof of Lemma 5: Let us first prove that the right hand side terms which appear in the expressions for $I_{\leq t}^\sigma[z]$ are indeed included in $I_{\leq t}^\sigma[z]$. If $a = 1$, consider a polynomial P of degree $\leq t$ of the form $P(z) = Q(z^\ell - b^{\ell-1}z)$ for some polynomial Q . We have:

$$\begin{aligned} P(z+b) &= Q\left((z+b)^\ell - b^{\ell-1}(z+b)\right) \\ &= Q\left(z^\ell + b^\ell - b^{\ell-1}z - b^\ell\right) \\ &= Q\left(z^\ell - b^{\ell-1}z\right) \\ &= P(z). \end{aligned}$$

We just used the fact that ℓ is the characteristic of \mathbb{F} and therefore $(z+b)^\ell = z^\ell + b^\ell$.

In the case $a \neq 1$, if we consider a polynomial P of degree $\leq t$ of the form $P(z) = Q((z - z_0)^\ell)$ for some polynomial Q of degree $\deg P/\ell$ we obtain:

$$\begin{aligned} P(az+b) &= Q\left((az+b - z_0)^\ell\right) \\ &= Q\left((az+b - az_0 - b)^\ell\right) \\ &= Q\left(a^\ell(z - z_0)^\ell\right) \\ &= Q\left((z - z_0)^\ell\right) \\ &= P(z). \end{aligned}$$

We used the fact that ℓ is also the order of a .

Let us prove now the reverse inclusion. Let P be a polynomial which is invariant by σ . Consider now a non constant polynomial R of smallest degree which is invariant by σ . Such a polynomial necessarily exists since the set of polynomials which are non constant and which are invariant by σ is non empty (since $z^\ell - b^{\ell-1}z$ in the case $a = 1$ and $(z - z_0)^\ell$ in the case $a \neq 1$, belong to it). Perform the division of P by R . We can write

$$P(z) = R(z)P_1(z) + P_2(z) \tag{10}$$

with $\deg P_2 < \deg R$. Observe now that

$$P(az+b) = R(az+b)P_1(az+b) + P_2(az+b). \tag{11}$$

Since $P(az + b) = P(z)$ and $R(az + b) = R(z)$ we deduce by subtracting the second equation to the first one, that we have

$$R(z) (P_1(az + b) - P_1(z)) = P_2(z) - P_2(az + b)$$

Since the degree of $S(z) \stackrel{\text{def}}{=} P_2(z) - P_2(az + b)$ is less than the degree of R , this can only happen if P_1 is invariant under σ and therefore also P_2 . Since R is a non constant polynomial of smallest degree which is invariant under σ and since $\deg P_2 < \deg R$, this implies that P_2 is constant. By carrying on this process (i.e. dividing P_1 by R) we eventually obtain that P is a polynomial in R . We finish the proof by proving that R can be chosen to be $R(z) = z^\ell - b^{\ell-1}z$ in the case $a = 1$ and $R(z) = (z - z_0)^\ell$ otherwise.

Let us first prove this for $a = 1$. We can add any constant to R , it will still be invariant under σ . We may therefore assume that $R(0) = 0$. We can also assume that R is monic. Let us observe now that $0 = R(0) = R(b) = R(2b) = \dots = R((\ell - 1)b)$ by the invariance of R under $z \mapsto z + b$. This implies that R is a multiple of $z(z - b) \dots (z - b(\ell - 1))$. R is therefore of degree greater than or equal to ℓ . The polynomial $z^\ell - b^{\ell-1}z$ is of degree ℓ , is invariant under σ and is a multiple of $z(z - b) \dots (z - b(\ell - 1))$. Therefore $R(z) = z^\ell - b^{\ell-1}z$.

Consider now the case $a \neq 1$. Without loss of generality (by adding a suitable constant as in the case $a = 0$) we may assume that $R(c) = 0$, where c is some element of \mathbb{F} such that the orbit of c under σ is of size ℓ . By the invariance of R under σ this implies that $0 = R(c) = R(\sigma(c)) = \dots = R(\sigma^{\ell-1}(c))$. This implies that $R(z)$ is divisible by $(z - c)(z - \sigma(c)) \dots (z - \sigma^{\ell-1}(c))$. Therefore R is of degree ℓ at least. Since $(z - z_0)^\ell$ is of degree ℓ and is invariant by σ we can choose $R(z) = (z - z_0)^\ell$. ■

This proves Proposition 4 when $\alpha = 1$. Let us prove now this proposition in general.

Proof of Proposition 4: Denote by σ the affine map $z \mapsto az + b$. First of all, let us notice that if there exists some polynomial $P(z)$ satisfying the equation $P(\sigma(z)) = \alpha P(z)$ for some α , then necessarily such an α satisfies $\alpha^\ell = 1$. This follows at once from the fact that we have $P(z) = P(\sigma^\ell(z)) = \alpha^\ell P(z)$. This also implies that the order of α divides ℓ . There are now two cases to consider.

Case $a = 1$: then the order ℓ of σ is necessarily equal to the characteristic of \mathbb{F} and there is no element, apart from 1, whose order divides ℓ . In this case, Lemma 5 implies Proposition 4.

Case $a \neq 1$: in such a case the order of a is equal to ℓ and a is a primitive ℓ -th root of unity. Since α is an ℓ -th root of unity, there exists in this case an integer d in the range $[0, \dots, \ell - 1]$ such that $\alpha = a^d$. Consider now a polynomial which is such that

$$P(\sigma(z)) = \alpha P(z). \quad (12)$$

If $\alpha = 1$, then we can use directly Lemma 5 and we are done. Otherwise, observe that from the fact that $\sigma(z_0) = z_0$ we deduce that

$$P(z_0) = P(\sigma(z_0)) = \alpha P(z_0).$$

This implies that $P(z_0) = 0$. Define now a polynomial P_1 by $P(z) = (z - z_0)P_1(z)$. Observe now that on the one hand

$$P(az + b) = (az + b - z_0)P_1(az + b) = a(z - z_0)P_1(az + b)$$

and that on the other hand

$$P(az + b) = \alpha P(z) = a^d(z - z_0)P_1(z).$$

Putting both equations together, we obtain

$$P_1(az + b) = a^{d-1}P_1(z)$$

If $d \neq 1$ we can carry on this process on P_1 , deduce from the previous equation that $P_1(z_0) = 0$ and deduce by induction on d that $P(z)$ has a zero of order at least d at z_0 and that the polynomial $P_d(z)$ defined by $P_d(z) = \frac{P(z)}{(z - z_0)^d}$ satisfies the equation

$$P_d(az + b) = P_d(z).$$

We apply Lemma 5 to P_d and derive from it that P should be of the form

$$P(z) = (z - z_0)^d Q \left((z - z_0)^\ell \right),$$

where Q is any polynomial of degree $\frac{\deg P - d}{\ell}$. Conversely, any polynomial P of this form is readily seen to verify (12). ■

B. Proof of Lemma 2

For this result, we will need the following lemma.

Lemma 6 $1^k + 2^k + \dots + (p-1)^k \equiv 0 \pmod{p}$ for every integer k which is not a multiple of $p-1$ whereas $1^k + 2^k + \dots + (p-1)^k \equiv -1 \pmod{p}$ otherwise.

Proof: Recall that the multiplicative group \mathbb{F}_p^\times is generated by a single element α which is of order $p-1$. The mapping

$$\begin{aligned} \phi_k : \mathbb{F}_p^\times &\rightarrow \mathbb{F}_p^\times \\ x &\mapsto x^k \end{aligned}$$

maps therefore \mathbb{F}_p^\times to a subgroup of \mathbb{F}_p^\times different from the trivial subgroup consisting only of 1 if and only if k is not a multiple of $p-1$. In other words, if k is a multiple of $p-1$, we have $s^k \equiv 1 \pmod{p}$ for any $s \in \{1, \dots, p-1\}$. This implies that $1^k + 2^k + \dots + (p-1)^k \equiv p-1 \equiv -1 \pmod{p}$. Assume now that k is not a multiple of $p-1$. Thus $\phi_k(\mathbb{F}_p^\times)$ is a subgroup of \mathbb{F}_p^\times of size a divisor $\ell > 1$ of $p-1$. Since \mathbb{F}_p^\times is generated by α , $\phi_k(\mathbb{F}_p^\times)$ is generated by $\beta \stackrel{\text{def}}{=} \alpha^k$ and we have

$$\begin{aligned} 1^k + 2^k + \dots + (p-1)^k &\equiv \frac{p-1}{\ell} (1 + \beta + \dots + \beta^{\ell-1}) \pmod{p} \\ &\equiv \frac{(p-1)(\beta^\ell - 1)}{\ell(\beta - 1)} \pmod{p} \\ &\equiv 0 \pmod{p} \end{aligned}$$
■

Let us prove now Lemma 2.

Proof: Let us first compute $S(z^t)$, where t is some nonnegative integer.

$$\begin{aligned} S(z^t) &= \sum_{s=0}^{p-1} (z + sb)^t = z^t + \sum_{s=1}^{p-1} \sum_{i=0}^t \binom{t}{i} z^{t-i} (sb)^i = \sum_{s=1}^{p-1} \sum_{i=1}^t \binom{t}{i} z^{t-i} (sb)^i \\ &= \sum_{i=1}^t b^i \binom{t}{i} \left(\sum_{s=1}^{p-1} s^i \right) z^{t-i} = \sum_{i=p-1}^t b^i \binom{t}{i} \left(\sum_{s=1}^{p-1} s^i \right) z^{t-i} \end{aligned} \quad (13)$$

where the last equation follows by using Lemma 6 which allows us to write $\sum_{s=1}^{p-1} s^i = 0$ when i is in the range $[1..p-2]$ and when the sum is performed over a field of characteristic p . This implies immediately that $S(\mathbb{F}_{\leq t}) \subseteq \mathbb{F}_{\leq t-p+1}[z]$. Since $S(Q(z))$ is obviously invariant by σ for any polynomial $Q(z) \in \mathbb{F}[z]$, we know from Lemma 5 that it is of the form $S(Q(z)) = R(z^p - b^{p-1}z)$ for some polynomial R in $\mathbb{F}[z]$. Its degree is therefore a multiple of p . This implies that we actually obtain the refined inclusion

$$S(\mathbb{F}_{\leq t}) \subseteq I_{\leq \lfloor \frac{t-p+1}{p} \rfloor_p}[z]. \quad (14)$$

Equality is proven by dimension considerations. It follows from Lemma 5 that $I_{\leq t}[z]$ is a vector space which is of dimension $\lfloor t/p \rfloor + 1$. The calculation (13) performed above also shows that $S(z^{(k+1)p-1})$ is a polynomial of degree kp (since the coefficient of z^{kp} which is equal to $b^{p-1} \binom{(k+1)p-1}{p-1} \sum_{s=1}^{p-1} s^{p-1}$ by (13) can be shown to be different from 0 by using the fact proven in Lemma 6 which says that $1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv -1 \pmod{p}$). This can be used to obtain that

$$\dim S(\mathbb{F}_{\leq t}) \geq \left\lfloor \frac{t-p+1}{p} \right\rfloor + 1 = \dim I_{\leq \lfloor \frac{t-p+1}{p} \rfloor_p}[z].$$

This together with (14) implies that

$$S(\mathbb{F}_{\leq t}) = I_{\leq \lfloor \frac{t-p+1}{p} \rfloor p} [x],$$

which concludes the proof. ■

C. Proof of Lemma 3

Proof: Let us calculate

$$\begin{aligned} S(z^t) &= \sum_{i=0}^{\ell-1} a^{di} (a^i(z - u_0))^t, \\ &= (z - u_0)^t \sum_{i=0}^{\ell-1} a^{(d+t)i}. \end{aligned}$$

This sum is equal to 0 as long as $d+t \not\equiv 0 \pmod{\ell}$ and is equal to $(\ell \bmod p)(z - u_0)^t$ when $d+t \equiv 0 \pmod{\ell}$. The polynomial $S(P(z))$ is therefore a polynomial of degree $\ell - d + \lfloor \frac{\deg P - \ell + d}{\ell} \rfloor \ell$ of the form

$$S(P(z)) = (z - u_0)^{t-d} \sum_{i=0}^{\lfloor \frac{\deg P - \ell + d}{\ell} \rfloor} a_i (z - u_0)^{i\ell} \quad (15)$$

when $\deg P \geq \ell - d$ and is equal to zero otherwise. We conclude the proof by noting that the term $\sum_{i=0}^{\lfloor \frac{\deg P - \ell + d}{\ell} \rfloor} a_i (z - u_0)^{i\ell}$ is a polynomial which is invariant by σ by Lemma 5. ■